Symantec Response to

Request for Information (RFI) for Arkansas Health Information Exchange (HIE)

May 7, 2010

Respondent Information

Company: Symantec Corporation, software vendor

Vendor Representative: Marc Potrzeboski, Sr. Agency Account Manager, Symantec

Marc_Potrzeboski@symantec.com

314-308-5898

Executive Summary:

Symantec produces a variety of COTS enterprise software solutions that are used extensively by public and private health IT entities. Our solutions are used to insure security and HIPAA privacy requirements, virtual workspaces for medical practitioners, high availability and disaster recovery of critical applications, and efficient storage and exchange of health information, including specialized solutions for PACS images.

These solutions are broadly deployed in Federal, State, and local government Health and Human Services agencies as well as with private provider and payers. Current users of these solutions include the U.S. Department of Health and Human Services Center for Medicaid Services, the State of Connecticut, Florida, Illinois, Michigan, Ohio, Kaiser Permanente, Mayo Clinic, Orlando Health System, Texas Children's Hospital, and many others.

As the world's largest security software vendor, Symantec has unique insight and capability to insure the availability, security, and privacy of HIE's. While we are not a provider of all core HIE functionality, we are responding to this RFI to make recommendations on best of breed solutions with augment health exchange. These include a solution to insure a sustainable HIE business model (use case 1) as well as optimal Security, Archiving, Back-Ups, and Disaster Recovery of the Arkansas HIE (use cases 2-6).

Our recommendations are summarized through five use cases are as follows:

1. Use Case: Create a sustainable HIE business model by offering a simple and cost-effective provider service around internet PACS archiving and exchange.

   Recommendation: Implement HIE technology which allows encrypted, compliant PACS images to be exchanged along with other PHI. PACS exchange solutions should be DICOM-compliant to insure compatibility with the variety of EMR solutions of HIE participants.

   Symantec's hosted PACS exchange would also provide Arkansas HIE a viable revenue stream, where the images could be hosted for providers at less than ½ the cost providers would pay to archive those images on local storage.

Hosting these PACS images in a Symantec cloud insures the security and recoverability from the vendor operating the world's largest storage cloud.

2. Use Case: Prevent loss of data by authorized users, resulting in a data breach. According to CMS, stolen or lost laptops, USB memory sticks, HDD's, and DVD's with unencrypted PHI has quickly become the most significant PHI data breach and this problem continues to grow.

   Recommendation: Extend role based access controls (RBAC) down to the data level. Protect the confidently of sensitive data and insure data is used appropriately based of sensitive data handling policies. Couple RBAC with data loss prevention solutions to identify, monitor, and manage PHI data use and to insure that all HIE data at-rest and-in motion is encrypted, as required by ONC's Meaningful Use rules.

3. Risk: Prevent non-compliance to HIPAA and Meaningful Use Security & Privacy rules, including security audit and logging.

   Recommendation: Automate compliance management and reporting. Document policies (HIPAA, NIST, state privacy, etc) on-line and have automated enforcement native to the HIE. Have the system capable of real-time HIPAA non-compliance alerts and on-demand compliance status reports which satisfy HIPAA and Meaningful Use audit requirements. Have the system include a robust audit trail on all PHI data access within the HIE. Leverage automated process controls to remediate HIPAA non-compliant findings to reduce operational risk and improve efficiently.

4. Use Case: Insure HIE participants (providers, payers, etc) require secure web access with two factor authentication application interfaces via the HIE.

   Recommendation: distribute all web applications to end-users via a single, highly secure, virtual workspace interface that protects user access and data security by only presenting authorized applications in a Secure Shell over an SSL/TLS session.

   Employ two factor authentication for secure information assurance and user authentication prior to virtual workspace authorization. Two factor authentication should use questions and answers to prove that the asserted identify of the individual is authentic to prevent fraud.

5. Risk: Inadequate managing & monitoring of the HIE "perimeter."

   Recommendation: HIE's have the requirement of 24X7 operations, highly sensitive information, but operated by a relatively small operating staff. The HIE must be diligent in monitoring security event logs and proactive in identifying and addressing emerging threats and vulnerabilities. To accomplish this, we recommend FHIN employ a 24X7 security monitoring and remediation service with real-time global security intelligence on emerging threats. This service could continuously correlate HIE network event logs and respond quickly to threats and vulnerabilities. It would relieve FHIN of the challenge to continuously employ, train, and staff 24X7 security specialists.

   Application profiles of the distinctive HIE applications would be created and correlated against the back-end global intelligence network (honeypot), to quickly assess 0-day vulnerabilities. This would increase threat awareness and allow HIE to test vendor patches based off risk of active threats taking advantage of vulnerability.

6. Use Case: Minimize the effects of a disaster and ensure HIE will be able to either maintain or quickly resume mission-critical IT functions, including providing access to its data and applications. Ideally, disaster recovery should include a fully replicated remote site as well as the ability for reliable, frequent or on-demand production disaster recovery testing of the primary site with solutions that do not disrupt the 24X7 operating environment.

   Recommendation: Utilize a remote failover site to fully replicate the HIE operating environment in the event of a catastrophic failure. Meet business recovery objectives by automating backup and recovery of HIE backbone and edge servers, application clustering, and data replication. A cross-platform clustering solution with automated failover and *zero downtime* disaster testing tools will minimize application downtime and maximize HIE beyond reactive recovery to proactive management of application availability.

   The HIE should utilize a backup solution that provides the ability to protect completely, store efficiently, recover anywhere, find easily and manage centrally.